DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

VOICE OF INDUSTRY DCSA MONTHLY NEWSLETTER

January 2022

Dear FSO (sent on behalf of your ISR),

This monthly newsletter contains recent information, policy guidance, and security education and training updates. Please let us know if you have any questions or recommendations for information to be included.

WHERE TO FIND THE "VOICE OF INDUSTRY" (VOI) NEWSLETTER

VOI Newsletters are posted for Facility Security Officers (FSOs) in the National Industrial Security System (NISS) Knowledge Base. Look for a monthly announcement on your NISS dashboard for each new VOI. VOI Newsletters are also found with important forms and guides on the Defense Counterintelligence and Security Agency (DCSA) website Industry Tools Page (VOIs are at the bottom). For more information on personnel vetting, industrial security, and other topics in the VOI, visit www.dcsa.mil.

TABLE OF CONTENTS

ENTERPRISE SECURITY OPERATIONS

CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM UPDATE

DCSA remains in Phase 1 and initial operating capability of its CUI Program Office and the implementation of its eight CUI responsibilities outlined in DoD Instruction 5200.48. To date, the DCSA CUI Program Office has developed and posted several resources to support Industry in developing CUI programs.

Resources include a CUI Slick Sheet, Frequently Asked Questions (FAQ), Quick Start Guide, and a DCSA Marking Job Aid. These products can be found on the DCSA CUI website, located at: Controlled Unclassified Information (dcsa.mil). DCSA has also made available a number of other resources at that page, including a CUI Quick Reference Guide, DoD CUI Marking Job Aid, CUI Cover Sheet, and the National Archives and Records Administration (NARA) CUI Marking Handbook.

DCSA is excited to be finalizing several additional resources to support Industry, which will soon be posted to the DCSA CUI website. These resources include:

- CUI Baseline Requirements - A list of five primary elements for Industry to establish a CUI program when performing on DoD contracts with CUI requirements.
- CUI Roadmap to Compliance - A visual job aid providing 11 key areas on which Industry can focus to become compliant with CUI requirements.
- CUI Standard Practices and Procedures (SPP) Template - A resource which CUI managers may find useful when establishing a CUI program resident within their facility or organization.
- CUI Training Reference Guide - A detailed reference guide outlining CUI training requirements.
- CUI Resources One-Pager - A list of CUI resources and associated web-links.
- CUI Glossary & Policy Summaries - A list of key CUI terms and relevant policies associated with CUI requirements.
- CUI Training Presentation - A sample training presentation that Industry can use to provide required CUI training to personnel.
- CUI Manager Customer Engagement Questions - A one-page script of questions to facilitate discussion between Industry and Government customers on CUI requirements.
- CUI Self-Inspection Tool for DoD and Industry - A comprehensive self-inspection tool that can be leveraged by both DoD and Industry to assess the effectiveness of an established CUI program.

SCIF ACCREDITATION MISSION TRANSFER UPDATE

DCSA continues to work closely with DIA on the SCIF accreditation mission transfer. In advance of formal mission transfer, DCSA will communicate to Industry via the VOI and other forums when Industry should start conferring with DCSA on SCIF-related matters. Until that time, Industry should continue to engage with their respective GCA and DIA on any SCIF-related matters.

FIELD OPERATIONS

THE NEW SECURITY REVIEW AND RATING PROCESS

The following paraphrases portions of an article in DCSA's Gatekeeper magazine. Please see DCSA's Gatekeeper magazine for the entire article entitled "New Rating Model Designed to Counter the Theft of Critical Program and Technologies."

On September 1, 2021, DCSA's Security Review and Rating Process (SRR) took effect. Security experts in the Critical Technology Protection (CTP) Directorate briefed Industry via live interactive webinars, answering questions on the ratings process, including new criteria to apply during security reviews.

In the SRR, compliance comes first. After a company is assessed as compliant and in general conformity with the NISPOM Rule, DCSA then looks beyond just "the person" (the FSO or security staff) to the "whole company approach" to gage the security culture, which includes management support, employee awareness, and cooperation within the security community. A formal security rating is then assigned to reflect contractor effectiveness in protecting classified information; superior, commendable, satisfactory, marginal, or unsatisfactory. The whole company's efforts are essential to reach high ratings.

Regarding the SRR, a Senior Industrial Security Representative deeply involved in development said, "We took the best practices from DiT [DCSA in Transition] and incorporated those into this methodology while making sure that we stay within the bounds of policy. It's a breath of fresh air for industry and agency personnel because it really does bring us back to what we do best, which is oversight and making sure that classified information and classified contract deliverables are being protected throughout their lifecycle."

Additionally, the CTP Operations Division Chief said, "Our partnership with industry is critical. This single security review model is an effort to provide industry with consistency and predictable engagements that they welcome. It's a valuable management tool and that's really what we're after —to stand shoulder-to-shoulder with Industry and get the absolute best results we can."

SECURITY VIOLATION PROCESS UPDATE

DCSA has recently completed an update to the security violation process, to include internal and external communications, terminology and templates. This has been conducted over a two-year period with SMEs throughout the agency, and coordinated with the military services. The goal of this effort was to align all processes and terminology to federal and DoD policies such as:

- 32 CFR Part 117, NISPOM Rule
- 32 CFR Part 2004, National Industrial Security Program
- DoDM 5200.01, Volume 3, DoD Information Security Program: Protection of Classified Information
- DoDM 5220.32, Volume 1, National Industrial Security Program: Industrial Security Procedures for Government Activities.

DCSA field personnel have been briefed and provided all updated materials to implement the new violation reporting process. In the near future, Industry will be provided with a comprehensive job aid that will aid in notification and mitigation of security violations, enabling better consistency, mitigation, and communication of results to the impacted Government Contracting Activities (GCAs).

BEWARE OF USB FLASH DRIVES IN THE MAIL

Since November 2021, ransomware groups have targeted U.S. cleared defense contractors via ground shipping mail. Bad actors are sending USB flash drives containing malicious code to lure companies to use them and infiltrate their information systems. Once recipients plug in the flash drive, the device executes a cyberattack, in which the flash drive registers itself as a keyboard and sends a series of preconfigured automated keystrokes to the user's device to gain administrative rights to install ransomware.

NEVER use a USB flash drive when you don't know its pedigree!

ALWAYS assume the worst and stay secure!

NATIONAL ACCESS ELSEWHERE SECURITY OVERSIGHT CENTER (NAESOC)

NAESOC: UPDATES, LINKS, AND MORE

See the NAESOC Web Page for the latest updates you will find in February:

FAQ Tab – Make things efficient as an FSO: downloadable NATO, COMSEC, and Critical Nuclear Weapons Design Information (CNWDI) briefings. The NAESOC has dedicated Counterintelligence support. What does that mean for you?

NAESOC Latest Tab – Learn about and sign up for this year's *Virtual DCSA Security Conference for Industry*. Sign up for CDSE's Monthly Security Newsletter

Reporting and Insider Threat Tabs – Just posted! A webex on counterintelligence reporting especially tailored for the NAESOC community. It's also good information and a useful resource for any cleared facility.

NATIONAL INDUSTRIAL SECURITY SYSTEM (NISS)

PSI REQUIREMENTS FOR INDUSTRY DATA COLLECTION THROUGH NISS

DCSA is responsible for projecting Personnel Security Investigations (PSI) requirements each year. The data collection for PSI projection requirements will be conducted March 7 through April 1, 2022, through the NISS Submission Site. Annual projections acquired from Industry through this collection are the key components in DoD program planning and budgeting for National Industrial Security Program (NISP) security clearances.

In preparation for this upcoming data collection, our Industry partners are highly encouraged to register for their NISS accounts before March 7, in order to participate in the survey. Registration instructions are found on the NISS Website under the Registration Tab.

We look forward to your participation. If you have any questions, please contact: dcsa.ncr.dcsa.mbx.psiprogram@mail.mil.

HAVE YOU SUBMITTED A CHANGE CONDITION PACKAGE?

Reminder: In accordance with Title 32 of The Code of Federal Regulations, Part 117, NISPOM Rule, Section 117.8(c)(7), cleared contractors are required to report certain changes affecting facility clearances to DCSA. These changes can involve one or more of the following:

- Ownership
- Legal Structure
- Operating Name
- Address
- Key Management Personnel (KMP)
- Foreign Ownership, Control or Influence (FOCI)

NOTE: The user guide for reporting a Change Condition can be found in the Knowledge Base under "Reporting a Change Condition Industry User Guide"

For any technical questions with NISS, please contact the DCSA Knowledge Center at 888-282-7682 and select Option 2, then Option 2. The DCSA Knowledge Center hours of operation are Monday through Friday from 8:00AM to 6:00PM EST.

DOD CONSOLIDATED ADJUDICATIONS FACILITY (DOD CAF)

REPORTING MENTAL HEALTH ISSUES ON YOUR E-QIP

Contrary to a common myth, reporting mental health issues on Section 21 of the SF-86 is not a "career-killer." In fact, a DCSA CAF analysis of denial and revocation statistics shows that only a fraction of one percent of adjudicative actions are denials or revocations solely based on psychological conditions.

There are at least two main reasons for this. Section 21 now has a greater focus on potential security-relevant concerns such as findings of mental incompetence, court-ordered care, psychiatric inpatient care, and certain conditions that may indicate judgment or reliability issues. Second, security professionals understand that when individuals candidly report their conditions and seek mental health care in accordance with their practitioner's recommendations, psychological conditions are not security concerns in the vast majority of cases.

That said, curiosity about how adjudicators resolve affirmative answers to Section 21 is understandable and the following offers some insight:

- After obtaining consent, a Background Investigator will conduct a brief interview with the applicant's treating health care practitioner focusing on whether the applicant's condition may impact his/her ability to perform sensitive national security duties.
- Depending upon the nature of the symptoms, more details may be obtained regarding treatment and prognosis.
- Psychologists that work with adjudicative teams may also request a review of pertinent medical records.

- If security concerns remain after these inquiries, the security professional may ask for the applicant to participate in an evaluation with a psychologist or psychiatrist who will consider possible security risks associated with the condition. Keep in mind that these security evaluations are quite rare. For NISP contractors, usually fewer than 300 evaluations a year are requested, and a majority of those determine the applicant's psychological condition does not present security concerns.

For more information please contact the DoD CAF Call Center at dcsa.meade.caf.mbx.call-center@mail.mil.

ASSISTANCE WITH SUPPLEMENTAL INFORMATION REQUESTS

DoD CAF has published guidance on responding to Supplemental Information Requests (SIRs). The Supplemental Information Request Instruction is a guide for our customers to respond to DoD CAF requests and to navigate the process to completion. The instructions guide you to "Claim the Task," use the calendar to enter the Acknowledgement Date, and complete. Once you click "Complete," the task will be moved to Task-In-Process, and you will need to access the task from your task inbox to work the SIR. Once you have completed the request by following the guidance instructions, you will click "Complete" with any required attachments included in the response. The full Supplemental Information Request Instruction is located here under Resources.

DOD CAF CALL CENTER

The DoD CAF Call Center is available by telephone or email for inquiries. Please contact us at 301-833-3850 or via email at DoD CAF Call Center. We look forward to hearing from you.

VETTING RISK OPERATIONS (VRO)

UPDATED INDUSTRY ENROLLMENT GUIDANCE

VRO continues to lead the effort to ensure that Industry's national security population is enrolled in a compliant Continuous Vetting (CV) program.

DCSA identified some subjects that were not enrolled post-adjudication since October 2021, and DCSA worked to enroll these subjects and update their enrollment information in DISS by January 15.

Post-adjudication enrollments after January 15 may take up to 30 days from the adjudication date. If enrollment has not occurred after 30 days, please submit a CSR-Supplemental in DISS requesting enrollment into CV.

VRO will analyze Industry CV enrollment data on a monthly basis and partner with internal and external stakeholders to ensure subjects are enrolled in CV. VRO will contact Industry partners over the next several months to review CV enrollment data and resolve any questions or issues.

For more information, please visit the Latest News Section on the DCSA website.

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE (CDSE)

JANUARY PULSE: CDSE SECURITY AWARENESS NEWSLETTER

We recently released the CDSE Pulse, a monthly security awareness newsletter that features topics of interest to the security community. In addition, we share upcoming courses, webinars, and conferences. The January newsletter focused on 2021 Year in Review. Check out all the newsletters in CDSE's Electronic Library or subscribe/update your current subscription to get the newsletter sent directly to your inbox by submitting your email address to CDSE News!

UPDATED CYBERSECURITY COURSES NOW AVAILABLE

Access CDSE's recently updated Cybersecurity courses:

- Applying Assessment & Authorization (A&A) in the National Industrial Security Program (NISP) (CS250.16)
- Introduction to the NISP RMF A&A Process (CS150.16)

The updates reflect policy changes involving the National to Institute of Standards and Technology (NIST) document and changes to the DCSA Assessment and Authorization Process Manual (DAAPM).

Visit CDSE eLearning Courses to view these updated products.

NEW COUNTERINTELLIGENCE SHORTS

Based on input from our annual curriculum review and a training needs analysis, CDSE developed four new shorts to assist security professionals.

- The Academic Solicitation Short enables the workforce to identify academic solicitation methods, determine countermeasures, and report suspicious activity.
- The Counterintelligence Concerns for National Security Adjudicators Short addresses counterintelligence concerns for adjudicators and explains concerns that may affect national security determinations.
- The Protecting Microelectronics Short considers what microelectronic are, DoD's microelectronic needs, existing threats, vulnerabilities, and associated reporting requirements.
- The Talking with Academia About Security Short informs Research Security, Counterintelligence Special Agents (CISAs), FSOs, and other security personnel working with scientists, engineers, and others in cleared academia about the unique challenges of talking to academics about security.

REGISTER NOW FOR UPCOMING WEBINARS

CDSE invites you to participate in all our upcoming Speaker Series:

- Classification of Information Released to the Public
  Wednesday, February 23, 2022
  1:00 – 2:00 p.m. ET

Visit CDSE Webinars to sign up for this event and join the discussion!

2022 VIRTUAL SECURITY CONFERENCE FOR INDUSTRY

There is still time to register for the 2022 Virtual DCSA Security Conference for Industry on February 16, 2022! This year's conference theme is "Inform & Transform: Enhancing the Security Landscape." The agenda will include updates on and changes to the Threat, Industrial Security, and Personnel Vetting programs, policies, and topics. The conference is open to cleared industry under the NISP.

Find out more and register at 2022 Virtual DCSA Security Conference for Industry.

SOCIAL MEDIA

Connect with us on social media!

DCSA Twitter: @DCSAgov

DCSA Facebook: @DCSAgov

CDSE Twitter: @TheCDSE

CDSE Facebook: @TheCDSE